CHAPTER B

Formal security proof for new SBHKAS

Here, we provide the proof for our proposed SBHKAS scheme given in Section 3.3 using the modern notions of security which would be the first provable security style proof for any dependent SBHKAS in the literature. Let $A_{SH}$ be the set of all nodes in the subscription hierarchy. Let $\text{Pred}(t_a, t_b)$ denotes the set of all nodes in the subscription hierarchy that can derive at least one leaf node $t$ with $t_a \leq t \leq t_b$. We can say that $\text{Pred}(t_a, t_b)$ is the set of all predecessor nodes in the subscription hierarchy, with respect to any of the leaf node with time slot from $t_a$ to $t_b$. $\text{Lower}(t_a, t_b)$ denotes the set of all the nodes with subscription interval $(t_c, t_d)$ such that $t_a \geq t_c$ and $t_b \geq t_d$. Let, $S_{(t_a, t_b)} = \text{Pred}(t_a, t_b) - \text{Lower}(t_a, t_b)$ represents set of nodes in $\text{Pred}(t_a, t_b)$ but not in $\text{Lower}(t_a, t_b)$. We define set $\text{corr}$ as set of secret keys known to the adversary in advance. Let, $\text{keys}(S)$ is the set of keys associated with the nodes in set $S$.

To prove the security of above scheme w.r.t. key recovery, we want to model all the information available to the adversary in advance. To achieve this, the game shown in Definition [key recovery] is played between the adversary and the challenger. Security of the scheme is bounded to arbitrary but fixed value in terms of security parameter.

**Theorem B.0.1.** Proposed scheme is secure w.r.t. key recovery against static adversary provided $h_{\text{pre}}$, assumption hold.

**Proof.** Let $G = (V, E)$ be some subscription hierarchy with $z$ time slots where $V$ is the set of nodes and $E$ is the set of edges in the hierarchy. Let, a subscription interval $(t_a, t_b)$ in the hierarchy and let, $A$ be a static polynomial time adversary
attacking the node $u_t$ with time interval $(t, t)$ with $t_a \leq t \leq t_b$. Now, based on Definition [key recovery], $A$ is having secret information corresponding to all unauthorized access nodes with subscription interval $(t_c, t_d)$ such that there does not exist a time slot $t$ with $t_a \leq t \leq t_b$ and $t_c \leq t \leq t_d$.

We consider three cases as follows where $|(t_a, t_b)|$ defines number of time slots in subscription interval $(t_a, t_b)$. First two cases are special cases and the third case is the general case. We show that all possible cases can be identified as one of the three cases defined below. Later, we prove that $KR$ adversary $A$ has a negligible advantage in finding the key of any node in the hierarchy as described one of the cases below and hence the overall maximum advantage of $A$ is negligible.

**Case 1:** $|(t_a, t_b)| = z$ i.e. $t_a = t_1$ and $t_b = t_z$.

As the Definition [collusion secure], there is no node $v$ with subscription interval $(t_c, t_d)$ is available such that there exists a time slot $t$ with $t_c \leq t \leq t_d$ and $t_1 \not\leq t \not\leq t_z$. Hence, this is trivial case where adversary can access only $Pub$ which contains public edge values with other public information.

We know that getting the key of any node in the subscription hierarchy will lead to knowing at least one of the encryption key in the hierarchy. Also, each node in the hierarchy can have only two type of edges; dependent edge without public value or edge with public value. Let us consider a preferable case from an adversary point of view, where a subscription node in the hierarchy has all incoming and outgoing edges with public edge values. We can argue that, if we are not able to get any non-negligible advantage in getting the key of a preferable node with the help of its all related public edge values in $Pub$ then it implies that same argument will follow for all the other nodes in the hierarchy. Hence, the advantage of getting any key in the hierarchy is negligible.

As a most preferable case, consider a subscription node $v$ in the hierarchy with $q$ incoming edges and 2 outgoing edges where every edge has one associated public edge value. Let $q$ edges between node $v$ and its immediate predeces-
sor nodes $u_1, u_2, ..., u_q$ has public edge values $r_{u_1,v}, r_{u_2,v}, ..., r_{u_q,v}$ respectively where $r_{u_i,v} = k_v \oplus h(K_{u_i,v})$ with $1 \leq i \leq q$. Similarly, let the public edge values between $v$ and its two immediate successor nodes $w_1$ and $w_1$ are $r_{v,w_1}$ and $r_{v,w_2}$ respectively with $r_{v,w_i} = k_{w_i} \oplus h(K_{v,l_{w_i}})$, $1 \leq i \leq 2$. We can see that, all $r_{i,j}$ public values corresponding to node $v$, has one distinct hash component. Therefore, no two public edge values will give any simplified solution to compute target key $K_v$. Hence, the adversary in game defined in Definition [Key Recovery] will not gain any non-negligible advantage in knowing any encryption key in the hierarchy. Hence, $KR$ advantage of the adversary $A$ against full subscription interval $(t_1, t_z)$ of $z$ time slots in the hierarchy is defined as,

$$Adv^{KR}_A(z) < \epsilon_{KR_z} \quad (1)$$

where $\epsilon_{KR_z}$ is negligible function of security parameter $\tau$.

**Case 2(a):** $|(t_a, t_b)| = z - 1$ with $t_a = t_2$ and $t_b = t_z$.

We can have two possible target subscription intervals with $|(t_a, t_b)| = z - 1$ as shown in Figure B.1. First, consider the target subscription interval $(t_2, t_z)$ (as shown in Figure B.1(a)), according to Definition [collusion secure] the adversary $A$ is given access to only subscription key $K_{(t_1,t_1)}$ (i.e. $A_{SH - Pred(t_2,t_z)}$). Figure B.1 shows partition of subscription nodes in the hierarchy into two sets: Set I and Set II. Set I contain nodes in set $A_{SH - Pred(t_2,t_z)}$ and Set II contain nodes in set $Pred(t_2,t_z)$.

![Figure B.1: Type of hierarchies in Case 2](image-url)
We assume that there exists a polynomial time adversary $A$ which can break the scheme with non-negligible probability. The probability of $A$ outputting correct key is same as the probability of which $h_{pre}$ problem can be broken as shown in lemma 1.

**Lemma B.0.1.** The advantage of $A$ in attacking target subscription interval $(t_2, t_z)$ is negligible.

**Proof.** Suppose that there exists an adversary $A$ that is able to compute a key $K_{(t_1,t_p)}$ with $p \geq 2$ (i.e. a node in set $S_{(t_2,t_z)}$) with non-negligible advantage. We construct a polynomial time adversary $A_{h_{pre}}$ that, on input $(h(), L, K_{(t_1,t_1)})$, uses the adversary $A$ to compute with non-negligible advantage the value $K_{(t_1,t_p)}$ where $h(L, K_{(t_1,t_p)}) = K_{(t_1,t_1)}$, as follows:

\[ A_{h_{pre}}(h(), L, K_{(t_1,t_1)}) \]

1. $A_{h_{pre}}$ knows key $K_{(t_1,t_1)}$ and it does not knows any key $K_{(t_1,t_q)}$ with $q \geq 2$. Let, $K_{(t_1,t_1)} = h_{l_{(t_1,t_1)}}(K_{(t_1,t_a)})$ with $q \geq 2$ where $L = l_{(t_1,t_1)}$.

2. Now there exists either a public edge value $r_{(t_1,t_a),(t_1,t_1)}$. $A_{h_{pre}}$ can compute $h_{l_{(t_1,t_1)}}(K_{(t_1,t_a)}) = K_{(t_1,t_1)} \oplus r_{(t_1,t_a),(t_1,t_1)}$.

3. Or if $K_{(t_1,t_1)}$ is dependent key then there exist a time slot $t_a$ with $a \geq 2$ such that $K_{(t_1,t_1)} = h_{l_{(t_1,t_1)}}(K_{(t_1,t_a)})$.

4. Let $K_{(t_1,t_a)}$ is the output of $A$ on input $(1^m, G, Pub, corr)$ where $corr = \{K_{(t_1,t_1)}\}$.

5. Output $K_{(t_1,t_a)}$.

Since, only way of getting $K_{(t_1,t_a)}$ from $K_{(t_1,t_1)}$ is by computing using $h_{l_{(t_1,t_1)}}(K_{(t_1,t_a)})$. So, we are able to construct an algorithm $A_{h_{pre}}$ which can break the $h_{pre}$ assumption with the same success probability as that of $A$ which was assumed earlier in the proof to have non-negligible probability. But, it is known that $h_{pre}$ assumption is hard and so success probability of $A$ with respect to subscription interval $(t_2, t_z)$ is also negligible. Hence,

\[ Adv^KR_A(t_2, t_z) < \epsilon_{KR_{z-1}} \] (2)
where $\epsilon_{KR_{z-1}}$ is negligible function of security parameter $\tau$.

\[\square\]

**Case 2(b):** $|(t_a, t_b)| = z - 1$ with $t_a = t_1$ and $t_b = t_{z-1}$.

In this case we consider the other target subscription interval with $|(t_a, t_b)| = z - 1$, i.e. $(t_1, t_{z-1})$ shown in Figure B.1(b). With the same reasoning as in case of subscription interval $(t_2, t_z)$ above, we can show that the success probability of $A$ in computing a key of any node in set $S_{(t_1, t_{z-1})}$ is negligible and hence,

$$Adv^A_{KR_{t_1, t_{z-1}}} < \epsilon_{KR_{z-1}}$$ (3)

where $\epsilon_{KR_{z-1}}$ is negligible function of security parameter $\tau$.

Combining equation (2) and (3),

$$Adv^A_{KR_{z-1}} \leq 2 \epsilon_{KR_{z-1}}$$ (4)

**Case 3: General case with $|(t_a, t_b)| < (z - 1)$.

In the general case we have either $t_a > t_1$ and/or $t_b < t_z$. Figure B.2 shows the general case graphically where hierarchy of nodes can be divided into three sets: set $I$, set $II$ and set $III$. Set $II$ in the middle represents set $Pred(t_a, t_b)$. Nodes in set $I$ and set $III$ represents the set $corr = keys(A_{SH} - Pred(t_a, t_b))$. If set $I$ exists, then we can consider this case as close to case 2(a) where now adversary have possession of more than one keys i.e. $Pred(t_1, t_{a-1})/Pred(t_a, t_z)$ for $a > 1$.

We assume that there exists a polynomial time adversary $A$ which can break the scheme with non-negligible probability. The probability of $A$ outputting correct key is same as the probability of which $h_{pre}$ problem can be broken as shown in lemma 2.

**Lemma B.0.2.** The advantage of $A$ in attacking target subscription interval $(t_a, t_b)$ is negligible.
Proof. Suppose that there exists an adversary $A$ that is able to compute a key $K_{(tc,td)}$ i.e. key of a node in set $S_{(ta, tb)}$ with non-negligible advantage. We construct a polynomial time adversary $A_{hpred}$ that, on input $(h(), L, K_{(tc,tf)})$ where key $K_{(tc,tf)}$ is known to $A$ (i.e. node $(tc,tf) \in S_{ta, tb}$), uses the adversary $A$ to compute with non-negligible advantage the value $K_{(tc,td)}$ where $h(L, K_{(tc,td)}) = K_{(tc,tf)}$, as follows:

$A_{hpred}(h(), L, S_{ta, tb})$

1. Let, $A_{hpred}$ knows key $K_{(tc,tf)}$ and it does not knows any key $K_{(tc,td)}$ with $(tc,td) \in S_{ta, tb}$. Let, $K_{(tc,tf)} = h_{(tc,tf)}(K_{(tc,td)})$ where $I_{(tc,tf)} = L$.

2. Now there exists either a public edge value $r_{(tc,td),(tc,tf)}$. $A_{hpred}$ can compute $h_{(tc,tf)}(K_{(tc,td)}) = K_{(tc,tf)} \oplus r_{(tc,td),(tc,tf)}$.

3. Or if $K_{(tc,tf)}$ is dependent key then there exist a node $(tc, td)$ with $(tc, td) \in S_{ta, tb}$ such that $K_{(tc,td)} = h_{(tc,tf)}(K_{(tc,td)})$.

4. Let $K_{(tc,td)}$ is the output of $A$ on input $(1^m, G, Pub, corr)$ where $corr = keys(set I) \cup keys(set III)$. 

5. Output $K_{(tc,td)}$.

Similarly, if set $III$ also exists along with set $I$, then we can consider this case as close to case 2(b) where now adversary have possession of additional keys i.e. $Pred(t_{b_1}, t_z) \setminus Pred(t_a, t_b)$ for $b < z - 1$. Now, the adversary knows the set of keys $corr = keys(set I) \cup keys(set III)$. Since, incoming edges to the nodes in set $III$ have similar types of relationship as the nodes in set $I$, we follow the same security argument as discussed in case of set $I$. 

Figure B.2: Type of hierarchies in Case 3
Since, only way of getting $K_{(t_c,t_d)}$ knowing $K_{(t_e,t_f)}$ is by computing $h_{I_{(t_e,t_f)}}(K_{(t_c,t_d)})$. So, we are able to construct an algorithm $A_{h_{pre}}$ which can break the $h_{pre}$ assumption with the same success probability as that of $A$ which was assumed earlier in the proof to have non-negligible probability. But, it is known that $h_{pre}$ assumption is hard and so success probability of $A$ with respect to subscription interval $(t_a, t_b)$ is also negligible. Hence,

$$Adv^K_A(t_a, t_b) < \epsilon_{KR|_{(t_a,t_b)}}$$ (5)

where $\epsilon_{KR|_{(t_a,t_b)}}$ is negligible function of security parameter $\tau$.

Let, there are $n$ number of such time intervals $(t_a, t_b)$, then we can combine all corresponding inequalities into one as shown below,

$$Adv^K_A(t_a, t_b) \leq \epsilon_{KRn}$$ (6)

where $\epsilon_{KRn}$ is addition of all $n$ negligible functions ($\epsilon_{KR|_{(t_a,t_b)}}$) and is again a negligible function of security parameter $\tau$.

Inequalities given in (1), (4) and (6) includes all possible subscription intervals in the hierarchy. Hence, adding right-hand side values of all these three inequalities gives maximum $KR$ advantage of the adversary $A$ against given subscription hierarchy of $z$ time slots

$$Adv^K_A \leq \epsilon_{KRz} + 2\epsilon_{KRz-1} + \epsilon_{KRn}$$

$$\leq \epsilon_{KR}$$ (7)

where $\epsilon_{KR}$ is negligible function of security parameter $\tau$. Hence the proposed scheme is secure against key recovery (KR).